REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application. Claims 3, 12, 19-20, 25-31, and 36 have been canceled. Claims 1-2, 4-11, 13-18, 21-24, 32-35, and 37-74 are pending, of which claims 1, 4-8, 11, 16, 23, 32, and 37-41 have been amended.

35 U.S.C. §112 Claim Rejections

Claims 11-12, 16, 19, and 38-40 are rejected under 35 U.S.C. §112, second paragraph (*Office Action* p.4). Appropriate amendments have been provided herein. Accordingly, Applicant respectfully requests that the §112 rejection be withdrawn.

35 U.S.C. §103 Claim Rejections

A. Claims 1-9, 32-37, 51, 60, and 65 are rejected under 35 U.S.C. §103(a) for obviousness over each of "Windows 2000, Server: Planning and Migration" to Deuby (hereinafter, "Deuby"), "Windows 2000, Active Directory Design and Deployment" to Olsen (hereinafter, "Olsen"), and "Windows NT/2000 Network Security" to Schultz (hereinafter, "Schultz") (*Office Action* p.6). Applicant respectfully traverses the rejection.

B. Claims 10-24, 38-50, 52-59, 61-64, and 66-74 are rejected under 35 U.S.C. §103(a) for obviousness over Deuby, Olsen, and Schultz in view of "Windows NT Server4 Security Handbook" to Hadfield (hereinafter, "Hadfield") (*Office Action* p.9). Applicant respectfully traverses the rejection.

Claim 1 recites an enterprise network architecture comprising ... "a trust link between a first network system root domain and a second network system root domain, the trust link configured to provide transitive resource access between the one or more first network system domains and the one or more second network system domains where the transitive resource access includes remote authentication such that an account managed by the second network system can initiate a request for authentication via a first network system domain."

The cited sections of Deuby, Olsen, and/or Schultz do not teach or suggest that "an account managed by the second network system can initiate a request for authentication via a first network system domain", as recited in claim 1.

In one example, Applicant describes (with reference to Fig. 2) that a user having an account managed by a domain controller 5 in forest *B* can logon and be authenticated via workstation 218 in forest *A*. A routing hint is determined that identifies the root domain of the trusted forest that manages the user's name (i.e., forest *B*), and the authentication request is referred along a trust path from forest *A* where the request originates to domain controller 5 in forest *B* that manages the account. (*Specification* p.27, lines 12-23).

As recited in claim 1, "an account managed by the second network system can initiate a request for authentication via a first network system domain". The Office cites to Deuby and Schultz which only describe domains that are linked by trust links in a domain tree, and that the domains share a common, contiguous namespace (*Deuby* p.66; *Schultz* p.184). Olsen illustrates a forest structure with "manual trusts connecting the forests" (*Olsen* p.102; Fig. 4.9).

The Office states that the links inherently allow connection to resources, and access to the resources requires authentication (*Office Action* p.8, ¶27). To the contrary, Schultz describes that such transitive trust is impossible (*Schultz* p.184), and Applicant describes that with conventional networked systems, it is difficult to manage a trust link across multiple forests because there is no provision to establish trust across different forest boundaries (*Background* p.3, lines 8-17). Except for manually established direct domain-to-domain trust links (as shown in Olsen), it is not possible to perform such tasks as accessing shared resources across multiple forest boundaries. Without being able to establish a trust link between multiple forests, it is not known where to route authentication and/or authorization requests that can be serviced by domains in other forests (*Background* p.3, lines 18-22).

As such, Applicant disagrees that any of the trust links in Deuby, Olsen, or Schultz inherently allow connection to resources across multiple forests, such as the autonomous network systems recited in claim 1. Further, there is no indication in any of Deuby, Olsen, and/or Schultz that "an account managed by the second network system can initiate a request for authentication via a first network system domain", as recited in claim 1.

Accordingly, claim 1 is allowable over Deuby, Olsen, and/or Schultz for at least the reasons described above, and Applicant respectfully requests that the §103 rejection be withdrawn.

Claims 2, 4-11, 13-18, and 21-24 are allowable by virtue of their dependency upon claim 1. Additionally, claims 10-11, 13-18, and 21-24 are also

allowable over Hadfield which does not address authentication across autonomous network systems. Some or all of claims 2, 4-11, 13-18, and 21-24 are also allowable over Deuby, Olsen, Schultz, and/or Hadfield for independent reasons. For example:

Claim 13 recites that "the first network system is configured to receive a request to logon to the second network system and determine from the trust link where to communicate the request, and wherein the second network system is configured to authenticate the request." None of the cited references teach or suggest that the first network system can determine from the trust link where to communicate the request, such as to the second network system, as recited in claim 13. Accordingly, the §103 rejection should be withdrawn.

Claim 32 recites a network system domain comprising ... "the trusted domain component being further configured to provide remote network authentication such that an account managed by a second network system domain can initiate a request for authentication via a network system domain in the first network system."

As described above in the response to the rejection of claim 1, Deuby, Olsen, and/or Schultz do not teach or suggest that "an account managed by a second network system domain can initiate a request for authentication via a network system domain in the first network system", as recited in claim 32. Accordingly, claim 32 is allowable over Deuby, Olsen, and/or Schultz for at least the reasons described above, and Applicant respectfully requests that the §103 rejection be withdrawn.

Claims 33-35 and 37-50 are allowable by virtue of their dependency upon claim 32. Additionally, claims 38-50 are also allowable over Hadfield which does not address authentication across autonomous network systems. Some or all of claims 33-35 and 37-50 are also allowable over Deuby, Olsen, Schultz, and/or Hadfield for independent reasons. Accordingly, the §103 rejection should be withdrawn.

Independent **Claims 51, 60, 65, 67, and 70** recite features that are allowable over Deuby, Olsen, Schultz, and/or Hadfield as described above in the response to the rejection of claims 1 and 32. The respective dependent claims 52-59, 61-64, 66, 68-69, and 71-74 are allowable by virtue of their dependency upon an allowable indcpendent claim. Accordingly, claims 51-74 are allowable over Deuby, Olsen, Schultz, and/or Hadfield, and Applicant respectfully requests that the §103 rejection be withdrawn.

Conclusion

Pending claims 1-2, 4-11, 13-18, 21-24, 32-35, and 37-74 are in condition for allowance. Applicant respectfully requests reconsideration and issuance of the subject application. If any issues remain that preclude issuance of this application, the Examiner is urged to contact the undersigned attorney before issuing a subsequent Action.

Respectfully Submitted,

Dated: Feb 16, 2006

By: _____

David A. Morasch
Lee & Hayes, PLLC
Reg. No. 42,905
(509) 324-9256 x 210